PATENT COOPERATION TREATY

PCT

REC'D 24 NOV 2004
WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PCT1909RK025jo	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP 03/09347	International filing date *(day/month/year)* 22.08.2003	Priority date *(day/month/year)* 30.08.2002
International Patent Classification (IPC) or both national classification and IPC H04L29/06		
Applicant ERRIKOS PITSOS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
30.03.2004	22.11.2004
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Lopez Monclus, I. Telephone No. +49 89 2399-7113

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 03/09347

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-14 as originally filed

Claims, Numbers

1-21 as originally filed

Drawings, Sheets

1/6-6/6 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-19, 21
	No:	Claims	20
Inventive step (IS)	Yes:	Claims	1-19, 21
	No:	Claims	20
Industrial applicability (IA)	Yes:	Claims	1-21
	No:	Claims	

2. Citations and explanations

   see separate sheet

Cited documents:

D1: US-A-6 055 236 (BORELLA MICHAEL S ET AL) 25 April 2000 (2000-04-25)
D2: EP-A-1 035 702 (SUN MICROSYSTEMS INC) 13 September 2000 (2000- 09-13)
D3: XP-000740492: "Internal Firewalls can protect subnetworks from unauthorized access") Ning Sun. COMPUTER TECHNOLOGY REVIEW, WESTWORLD PRODUCTION CO. LOS ANGELES, US. 01-06-1997

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement.

1. Independent claim 20 is formulated in such broad terms that its subject matter appears to be entirely anticipated by the content of document D1. Therefore the subject-matter of independent claim 20 is not new in the sense of Article 33(2) PCT. Indeed document D1 discloses, according to all the features of claim 20,

a public key server comprising:
storage means for storing information in regard to a public key;
a public key request interface for receiving a request for public key information stored in said public key information storage means and transmitting the requested information to a requesting device in response thereto (Column 35, lines 12-22: " In one exemplary preferred embodiment of the present invention, at Step 346, the digital certificate is published in a location accessible to external network devices on external networks 30. In order for an external network device to use the certificate, it is published in a way that allows the external network device to retrieve it. For example, it might be stored in a Lightweight Directory Access Protocol ("LDAP") directory under a name representing the service. Other storage options are also possible, such as storing the digital certificates in a public file, in a public database or on a network server are accessible to the external network");

wherein said storage means stores a public network address of a gateway as a destination address of data to be transmitted to a recipient, for gateways identifying the recipient by means of a public key identifier included in the transmitted data and forwarding the data to the recipient; and said public key request interface is adapted to transmit said stored public network gateway address to the requesting device (Column 5, lines 11-25: "The digital certificate includes a network address valid outside an internal distributed network address translation network, service name, service parameters and an optional public encryption key. One or more of the service parameters may be obtained with a Port Allocation Protocol used for distributed network address translation. The digital certificate is signed with a secure digital signature. The digital certificate is published in a location on the internal network accessible to external network devices on external networks. The digital certificate is used by an external network device to request a desired service from an internal network device on the internal distributed network address translation network. In one exemplary preferred embodiment of the present invention, the digital certificate is a public encryption key certificate for an Internet Protocol security service.").

Furthermore, it should be noted that even if novelty of claim 20 could be argued, based on minor differences between the features of claim 20 and those disclosed in D1, the subject matter of claim 1 would not involve an inventive step, Article 33(3), having regard to the disclosure of D1 as this document discloses the same object and the same type of solution as the present application.

2. The subject-matter of the independent claims 1, 14 and 21 meets the requirements of Article 33 (1), (2) and (3) PCT regarding novelty and inventive step.

These claims relate to a gateway (independent claim 1), a system (independent claim 14) and a method (independent claim 21) for transmitting data between a remote device in a public network and an internal device in an internal network using asymmetric keys.

The closest prior art is the US Patent 6055236, which describes a method for allowing services to be identified and requested on an internal distributed network address translation network. Each internal network device requests from the router a set of locally unique ports for external communication with external devices. Ephemeral ports are replaced by a combination network address including a locally unique port and a common external network address.

The problem with the method disclosed in the US Patent 6055236 is that the network address translation using locally unique ports for external communication with external devices, particularly by using a fixed port mapping of internal devices maintained by the router, implies that the position and configuration of internal services and devices has to be fixed. It is therefore not optimized with regard to the number of required addresses.

In contrast the present invention does not require fixed IP addresses and fixed port mappings that have to be included as additional payload in a certificate for identifying internal devices of an internal network. Instead, the present independent claims teach that the destination of incoming data that is addressed to the gateway can be identified using public key information. Such public key information may already be included in a certificate and thus, no additional payload has to be included and no additional unique identifiers, such as a fixed port allocation, have to be generated and maintained for this purpose.

Claims 1, 14 and 21 disclose a gateway, a system and a method which uses public key identifiers for identifying the internal destination of received data reusing said data field and avoiding additional data to be determined. The number of IP addresses is reduced by using a gateway forwarding data to an internal device based on a public key information (which is globally unique) included in the transmitted data for identifying the internal device.

There is no indication of this solution in neither US Patent 6055236 nor in the other 7 documents listed in the European Search Report. US Patent 6055236 discloses the usage of a SPI (Security Parameter Index)-to-internal network address table in Fig. 21, but it is not used to identify the address of the internal

devices, but to identify the SPI values when being presented with the internal network address of these devices. The identification of the internal destination device of incoming data by the router is however completely unrelated to the SPI values stored in the table shown in FIG. 21. In fact, these values are only used for establishing a secure connection between an external device and an internal device, i.e. after the router has established the connection.

Therefore, the subject-matter of present claims 1, 14 and 21 is considered to be novel and inventive.

3. Claims 2-13 and 15-19 are dependent from claims 1 and 14 and comply therefore with the requirements of Article 33 (1), (2) and (3) PCT.

4. The independent claims are not properly cast in the two-part form, with those features which in combination are part of the prior art (see document D1), being placed in the preamble (Rule 6.3(b) PCT).

5. Documents D1-D3 have not been identified in the description and the relevant background art disclosed therein was not briefly discussed (Rule 5.1(a)(ii) PCT).

6. Reference signs in parentheses are not inserted in the claims to increase their intelligibility, Rule 6.2(b) PCT. This applies to both the preamble and characterising portion.

7. Following from the disclosure of documents D1-D3, the statement indicating the technical problem to be solved by the invention was not revised.

8. Independent claims 1,14 and 20 do not meet the requirements of Article 6 PCT in that it is not clear which category the claims are referring to.

   In this case of claims containing both process and apparatus features, the applicant is asked to amend the claims in such a way that it is clearly in one or the other category.

   In this connection, functional features used to define physical entities (e.g. "means for..." of "means arranged in such a way as to...") should be interpreted as features of an apparatus whereas features relating to activities in which the use of a physical entity is implied (e.g. doing something by means of) should be regarded as features of a process.

9. Claim 21 is not clear due to what seems to be a clerical error: "..in a gateway of the internal device..." (lines 3 and 6) should presumably read "...in a gateway of the internal network...".

10. It has to be said that description pages 13 and 14, figure 11 and claims 7-13, 18 and 19 introduce subject-matter which extends beyond the content of the priority document pertaining to the present application (Article 19(2) PCT). Hence, since claims 7-13, 18 and 19 are based on description pages 13 and 14, they don't enjoy priority rights from the filing date of the priority document.